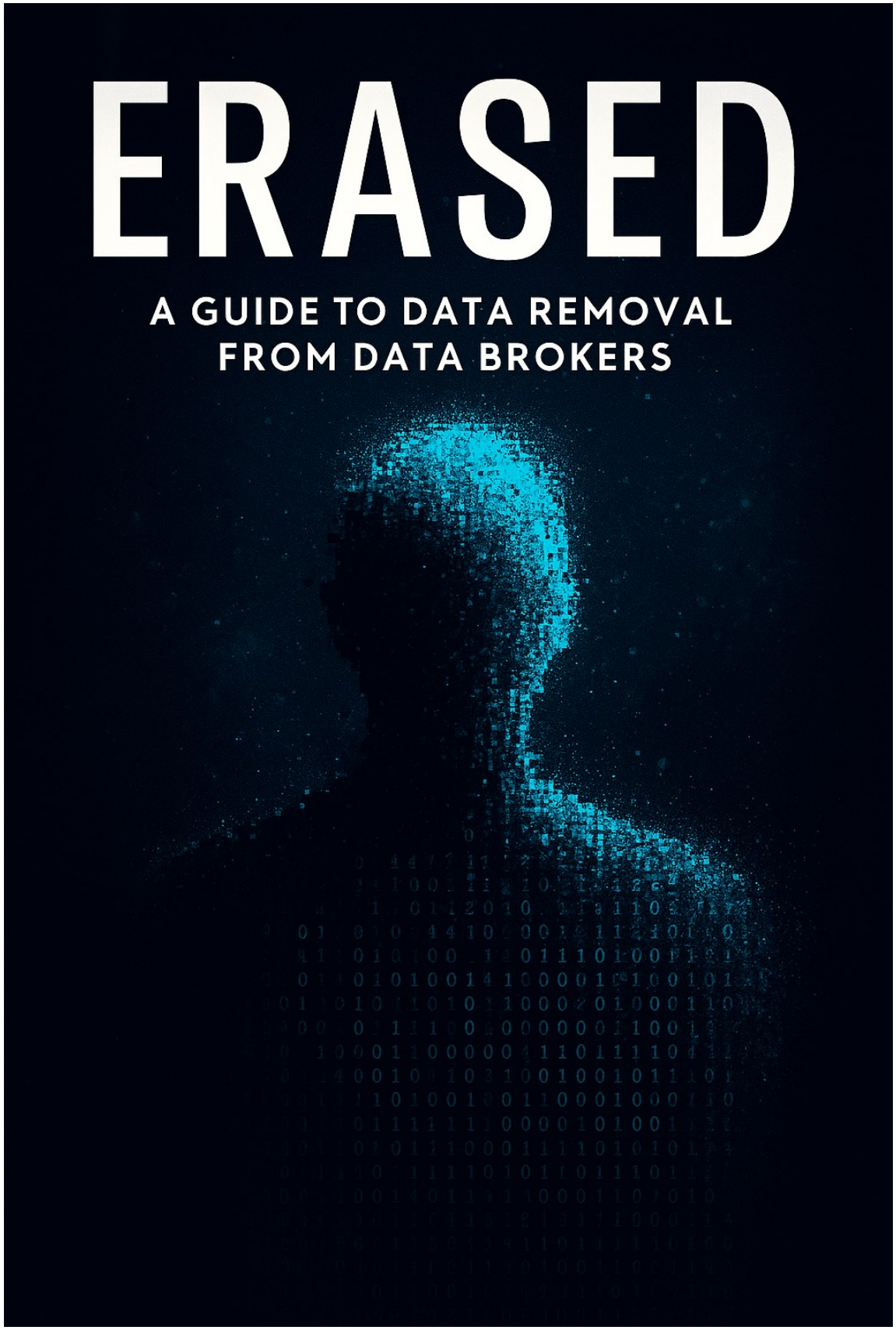
ERASED
A GUIDE TO DATA REMOVAL
FROM DATA BROKERS

TABLE OF CONTENTS

- UNDERSTANDING DATA BROKERS
- THE RISKS OF EXPOSURE
- MAPPING YOUR DIGITAL FOOTPRINT
- MANUAL OPT-OUT STRATEGIES
- AUTOMATED DATA REMOVAL SERVICES
- LEGAL PROTECTIONS AND LIMITATIONS

CHAPTER 1
UNDERSTANDING DATA BROKERS

"A must-read for anyone serious about online privacy."
— Cybersecurity Today

Erased: A Guide to Data Removal from Data Brokers

📖 Introduction

In the digital age, personal data is currency—and data brokers are the banks. These entities collect, trade, and monetize your information, often without your knowledge or consent. This book is your roadmap to reclaiming your privacy.

🕵️ Chapter 1: Understanding Data Brokers

Data brokers are companies that collect personal information about individuals and sell it to third parties. This data can include everything from your name, address, and phone number to your shopping habits, online activity, and even political affiliations. They operate behind the scenes, aggregating data from public records, online cookies, social media platforms, and commercial transactions.

Types of Data Brokers:

- **Marketing brokers**: Focus on consumer behavior to help companies target ads.
- **People search brokers**: Provide detailed personal profiles for public lookup.
- **Risk mitigation brokers**: Assist in fraud detection and background checks.

Understanding how data brokers operate is the first step toward reclaiming control.

⚠️ Chapter 2: The Risks of Exposure

When your personal data is widely available, it opens the door to serious risks:

- **Identity theft**
- **Stalking and harassment**
- **Unwanted marketing**
- **Discrimination**

Case Study:

Jane Doe discovered her home address and phone number listed on multiple people search sites. After receiving threatening calls, she used manual opt-out strategies to remove her data and regained peace of mind.

🧭 Chapter 3: Mapping Your Digital Footprint

To begin removing your data, you must first know where it lives. Start by Googling your name, phone number, and address. Look for profiles on sites like Spokeo, Whitepages, and MyLife.

Helpful Tools:

- Mozilla Monitor

- McAfee Personal Data Cleanup
- OneRep

Create a spreadsheet to track where your data appears and what actions you've taken.

📝 Chapter 4: Manual Opt-Out Strategies

Manual removal is time-consuming but effective. Here's how:

1. Visit the broker's website.
2. Locate the opt-out form.
3. Submit your request.
4. Track your progress.

Sample Opt-Out Template:

```
 Subject: Opt-Out Request
To Whom It May Concern,
I am requesting the removal of my personal information from your website. Please remove all data associated with:
Name: [Your Name]
Address: [Your Address]
Email: [Your Email]
Phone: [Your Phone Number]
Thank you,
[Your Name]
```

🤖 Chapter 5: Automated Data Removal Services

If manual removal feels overwhelming, consider automation:

Service	Coverage	Cost (Annual)	Monitoring
Incogni	130+ sites	$77	Yes
DeleteMe	30+ sites	$129	Yes
OneRep	100+ sites	$99	Yes

Choose based on your budget, coverage needs, and desired level of control.

⚖️ Chapter 6: Legal Protections and Limitations

Privacy laws vary by region:

- **CCPA (California)**

- **GDPR (EU)**
- **Other U.S. states**

You can file complaints with:

- FTC
- State Attorney General's Office

Limitations: Many laws only apply to residents of specific regions, and enforcement can be slow.

🔒 Chapter 7: Preventing Future Exposure

Once your data is removed, keep it protected:

- Use privacy-focused browsers
- Install tracker blockers
- Use a VPN
- Limit social media sharing
- Read terms and conditions

Visual:

Diagram showing a "Privacy Shield" with layers like VPN, browser settings, and social media controls.

💡 Chapter 8: Case Studies and Success Stories

Mark used DeleteMe to remove his data and saw a 90% reduction in spam calls. **Angela**, a domestic violence survivor, manually removed her data to protect her location. **Carlos**, a small business owner, used OneRep to clean his online presence before launching a new brand.

Lessons:

- Persistence pays off
- Combine manual and automated strategies
- Stay informed about new broker sites

✅ Conclusion: Reclaiming Your Digital Identity

Data removal is not a one-time fix—it's an ongoing commitment to privacy. With the right tools and knowledge, you can take back control and protect your digital self.

Checklist:

- [ ] Search for your data online

- [ ] Use opt-out forms or services
- [ ] Monitor your digital footprint
- [ ] Practice privacy-first habits
- [ ] Stay updated on laws and tools

Large data aggregators and credit bureaus

These companies collect vast amounts of data used for marketing, financial services, and risk assessment.

Acxiom

CoreLogic

Equifax

Experian

LexisNexis

Oracle America, Inc. (Oracle Cloud Data)

TransUnion

People-search sites

These sites compile personal information from public records and other sources and sell it to individuals and businesses for background checks or other purposes.

411.com

BeenVerified

Intelius

Instant Checkmate

MyLife

Nuwber

PeekYou

PeopleFinders

PeopleLooker

Pipl

Radaris

Spokeo

TruthFinder

Whitepages

Marketing and advertising data brokers

These companies specialize in selling information to advertisers for targeted marketing campaigns.

Epsilon

FullContact

Gravy Analytics

LiveRamp (owned by Acxiom)

Lusha

Merkle

Mobilewalla

Tapad

ZoomInfo

How to protect your data

While it is nearly impossible to prevent all data collection, you can take steps to reduce your exposure to data brokers.

Opt-out requests: You can manually contact data broker sites individually and ask them to remove your information. This can be a time-consuming and ongoing process.

Automated removal services: Paid services like **Aura**, **DeleteMe**, **Incogni**, and **Optery** automate the opt-out process for you by submitting deletion requests to many brokers.

Use privacy tools: Install browser extensions that block web trackers and use a **Virtual Private Network (VPN)** to mask your online activity.

Check app and website settings: Review privacy settings on websites and mobile apps to see what information they collect and share with third parties.

Freeze your credit: Placing a credit freeze with the major credit bureaus (**Equifax**, **Experian**, and **TransUnion**) is a proactive measure against identity theft.

Limit online sharing: Be cautious about providing personal details in online quizzes, surveys, and on social media.

Decrypting the shadows
of stolen data...

There are many options for protecting your personal data, from basic security practices to using specialized software. A comprehensive approach involves a combination of account management, online activity protection, and proactive data removal.

Manage your online accounts and passwords

Use strong and unique passwords: Never use the same password for more than one account. Create passwords that are at least 15 characters long and combine uppercase and lowercase letters, numbers, and symbols.

Utilize a password manager: These tools can generate, store, and auto-fill strong, unique passwords for all your online accounts, so you only have to remember one master password.

Enable two-factor authentication (2FA): Also known as multi-factor authentication, 2FA requires a second form of verification to log in, such as a code sent to your phone. This adds a critical layer of security even if your password is stolen.

Close old accounts: If you have old email addresses, social media profiles, or customer accounts you no longer use, close them. This reduces the number of potential entry points for hackers and data brokers.

Watch for phishing attempts: Be skeptical of any unsolicited email, text, or phone call that asks for personal or financial information. Never click on suspicious links or download attachments from unknown senders.

Protect your internet activity

Use a **VPN: A Virtual Private Network (VPN)** encrypts your internet traffic and masks your IP address. This is especially important when using public Wi-Fi networks, which are often unsecured.

Secure your home Wi-Fi: Always use a strong, unique password for your home wireless network. Also, consider setting up a **Virtual Local Area Network (VLAN)** to add another layer of security.

Keep software and devices updated: Enable automatic updates for your computer's operating system, apps, and browsers. These updates often include critical security patches to fix newly discovered vulnerabilities.

Control app permissions: On your smartphone and other devices, review the permissions for each app. If a flashlight app wants access to your contacts, for example, deny the request or delete the app.

Browse safely: When entering sensitive information, such as financial data, on a website, ensure the web address begins with https:// and shows a closed padlock icon.

Prevent data broker collection

Limit social media sharing: Be mindful of what you share publicly online. Even seemingly harmless information, like your birthday or hometown, can be used by data brokers or hackers.

Adjust privacy settings: Regularly review and customize the privacy settings on social media platforms and in your Google Account.

Opt-out of data collection: Contact data brokers and people-search sites directly to request the removal of your personal information. This can be time-consuming and often requires regular follow-ups.

Use a data removal service: Services like **DeleteMe**, **Incogni**, and **Optery** can automate the process of sending opt-out requests to hundreds of data brokers on your behalf.

Safeguard your personal identification numbers (PINs)

Do not carry your Social Security card: Keep your card and any other documents containing sensitive numbers in a secure place at home. Do not carry them in your wallet.

Be cautious with your PINs: Memorize your PINs and do not write them down or share them with others. Do not use your PIN for anything else.

What to do if your data is leaked

Check for leaks: Use a service like **Have I Been Pwned (https://haveibeenpwned.com/)** to see if your email address has appeared in a data breach.

Set up fraud alerts and credit freezes: Place a fraud alert or credit freeze with all three major credit bureaus (**Equifax, Experian**, and **TransUnion**). This prevents new credit accounts from being opened in your name without your express permission.

Monitor your credit reports: Check your credit report annually for suspicious activity.

PRIVATE
INVESTIBELOR

YOUR DATA IS BEING SOLD.
RECLAIM IT.

In ERASED, discover how data brokers harvest your personal information—and how you can fight back. Learn to track your digital footprint, opt out manually or automatically, and shield your identity from future exposure.

"A must-read for anyone serious about online privacy."
— Cybersecurity Today

'A must-read for anyone serious about online privacy.'